IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA *v.* ROBERT PURBECK A.K.A. "LIFELOCK" A.K.A. "STUDMASTER" A.K.A. "STUDMASTER1"	Criminal Action No. 3:21-cr-004-TCB-RGV

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS SEARCHES OF IPHONES

The United States of America, by Ryan K. Buchanan, United States Attorney, Michael Herskowitz, Nathan P. Kitchens, and Alex R. Sistla, Assistant United States Attorneys for the Northern District of Georgia, and Brian Z. Mund, Trial Attorney of the Department of Justice's Computer Crime and Intellectual Property Section, files this response in opposition to Defendant Robert Purbeck's ("Purbeck") Motion to Suppress 2023 Searches of iPhones. (Doc 99).

Introduction

In his recently-filed motion to suppress, Purbeck argues that an unpublished per curiam opinion issued in November 2022 seismically changed 11th Circuit law such that the Government must seize *and extract* forensic data—including from encrypted and password protected devices—within 14 days of the issuance of a search warant. (Doc. 99.) Purbeck's reliance on this case and his argument is misplaced. Under settled precedent, the search warrant, including for the iPhones here, was deemed executed when the devices were seized from his

Idaho home in August 2019. This makes sense—otherwise, law enforcement would be racing a two-week deadline to defeat password protection and encryption for any number of devices seized during the execution of a lawful search warrant. Further, Purbeck's challenge to the reasonableness of the Government's review of these password-protected iPhones is untimely and waived. But even if Purbeck's argument had merit, which it does not, suppression is not the appropriate remedy. For these reasons, which will be developed further below, Purbeck's motion should be denied without an evidentiary hearing.

Procedural History

On March 2, 2021, a Grand Jury sitting in the Northern District of Georgia returned an indictment charging Purbeck with wire fraud, access device fraud, and computer fraud and abuse in connection with a series of computer intrusions against medical practices in Georgia, the City of Newnan, and an orthodontist in Wellington, Florida. (Doc. 1.) On December 13, 2021, Purbeck filed a motion to suppress statements and password disclosures (Doc. 25), a motion to suppress the search and seizure of evidence from his residence (Doc. 26), a motion to suppress email searches (Doc. 27), and a motion to dismiss for lack of venue. (Doc. 30.)

On September 1 and 2, 2022, U.S. Magistrate Judge Russell G. Vineyard held an evidentiary hearing on Purbeck's motion to suppress statements and password disclosures. (Doc. 64.) On February 13, 2023, Purbeck filed his post-hearing brief; the Government filed its response brief on March 15, 2023, and Purbeck filed his reply on April 11, 2023. (Docs. 80, 82, 85.) On May 18, 2023,

Judge Vineyard issued a Report and Recommendation, recommending that Purbeck's motions to dismiss and suppress be denied. (Doc. 87.) On June 26, 2023, Purbeck filed objections to the Report and Recommendation. (Doc. 92.)

On July 20, 2023, Purbeck moved for leave to file a supplemental motion to suppress evidence from two iPhones that the Government had just recently decrypted. (Doc. 95.) On July 26, 2023, United States District Judge Timothy C. Batten, Sr., adopted the Report and Recommendation and referred Purbeck's pending motion for leave to file a supplemental motion to suppress to Judge Vineyard. (Doc. 96.) Also, on July 26, 2023, Purbeck filed an additional motion for leave to file another supplemental motion to suppress, this one for nearly all of the evidence recovered in the searches of computers, phones, hard drives, and storage devices seized pursuant to an August 2019 search warrant for Purbeck's Idaho residence. (Doc. 97.)

Following a telephone conference with the parties on August 2, 2023, Judge Vineyard granted Purbeck's motion for leave to file the motion to suppress the 2023 searches of the iPhones. (Doc. 98.) During the telephone conference, Government counsel stated it did not oppose the motion for leave to file the motion to suppress, while reserving the right to oppose the merits of the motion and its timeliness. Purbeck's motion to suppress the searches of the iPhones was filed on the docket later the same day. (Doc. 99.)

The Government's response, due on September 7, 2023, is set forth herein.

Statement of Facts

On August 19, 2019, United States Magistrate Judge Ronald Bush in the District of Idaho signed a search warrant for the premises of Purbeck's residence, located in Meridian, Idaho. (Doc. 87 at 67–68.) Two days later, on August 21, 2019, the Federal Bureau of Investigation ("FBI") executed the search warrant at Purbeck's residence, and lawfully seized a large number of devices and electronically stored data, including computer equipment, electronic storage devices, cell phones, and other items, including the iPhone 7 and iPhone 8 at issue in Purbeck's present motion to suppress.[1]

After the warrant was executed, the FBI prioritized the review of the voluminous evidence, starting with the devices for which Purbeck had provided passcodes. Until about late 2020 or early 2021, Purbeck was cooperating with the Government's investigation and the parties were attempting to resolve the case.[2] During this time, on or about December 23, 2020, the FBI attempted unsuccessfully to extract the contents of the two iPhones.

On about June 24, 2021, the FBI again attempted to bypass the encryption on the iPhone 7. By September 7, 2022, based on the difficulties accessing the iPhones, the FBI requested technical assistance from forensic examiners with FBI's Computer Analysis Response Team ("CART"). Due to resource limitations and a backlog in assistance requests from authorities throughout the state of

---

[1] The FBI executed the search warrant well before the deadline of August 30, 2019, as required on the face of the warrant.

[2] Indeed, Purbeck traveled to Atlanta for a proffer with the FBI in the months following the execution of the warrant.

Georgia, FBI CART initiated its attempts to bypass the iPhone encryption on or around May 30, 2023. (Docs. 95-2, 95-3.) FBI CART was able to successfully bypass the encryption on or about June 6, 2023. (*Id.*) The Government then notified Purbeck's counsel on or about June 22, 2023, that it had recently unlocked the two iPhones and wanted to produce images of the phones to Purbeck as part of its ongoing discovery obligations. After receiving a blank hard drive from Purbeck's counsel, the Government promptly produced forensic images of the iPhones on or about July 7, 2023.

Argument

A. Under settled federal law, the search warrant was executed when Purbeck's devices were seized.

The gravamen of Purbeck's motion to suppress is that the Government failed to execute the search warrant on the iPhones within fourteen days of issuance of the search warrant, in violation of Federal Rule of Criminal Procedure 41. (Doc. 99 at 3.) Purbeck's argument is misplaced and frankly illogical.

Rule 41(e)(2)(A) provides that a "warrant must command the officer to . . . execute the warrant within a specified time no longer than 14 days." Fed. R. Crim. P. 41. Rule 41(e)(2)(B) provides in relevant part that for warrants authorizing the seizure of electronic storage media or electronically stored information, "[t]he time for executing the warrant in Rule 41(e)(2)(A) . . . refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." As the accompanying advisory committee notes explain, "[Rule 41(e)(2)] acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine

what electronically stored information falls within the scope of the warrant. . . . [T]he Rule limits the . . 14[] day execution period to the actual execution of the warrant and the on-site activity." Fed. R. Crim. P. 41(e)(2), Advisory Committee Note, 2009 Amendments;[3] *see also United States v. Dixon*, No. 320CR00003TCBRGV, 2021 WL 2327063, at *5 (N.D. Ga. Apr. 15, 2021), *report and recommendation adopted*, No. 3:20-CR-3-TCB, 2021 WL 1976679 (N.D. Ga. May 18, 2021) ("Rule 41(e) expressly authorizes the later review of electronically stored information contained within an item seized during the 14-day time period . . ."); *United States v. Mobely*, No. 116CR145TWTJKL6, 2017 WL 10574358, at *11 (N.D. Ga. Oct. 26, 2017), *report and recommendation adopted*, No. 1:16-CR-145-6-TWT, 2018 WL 5077755 (N.D. Ga. Oct. 18, 2018); *United States v. Alston*, No. 15 CR. 435 (CM), 2016 WL 2609521, at *3 (S.D.N.Y. Apr. 29, 2016) ("[I]t is clear from the language of the Advisory Committee Notes that the 14 day limit applies only to 'the actual execution of the warrant and the on-site activity,' (in this case, the seizure of the iPhone) and not to 'any subsequent off-site copying or review of the media or electronically stored information.'").

Thus, a warrant authorizing the search and seizure of electronic evidence is executed when a device is *seized from the premises*. And with good reason: "To conclude otherwise would be to allow law enforcement's lawful, permitted access to cellphone data to be undercut in any case where a password prevents

[3] "While not binding, [the Eleventh Circuit] recognize[s] that advisory committee notes are 'accorded great weight' in interpreting federal rules." *United States v. Vedrine*, No. 20-13259, 2022 WL 17259152, at *6 n.7 (11th Cir. Nov. 29, 2022) (citing *Horenkamp v. Van Winkle and Co., Inc.*, 402 F.3d 1129, 1132 (11th Cir. 2005).)

law enforcement from immediately accessing the data it is permitted to seize. That is not the law." *United States v. Whipple*, No. 3:20-CR-31-KAC-JEM, 2022 WL 3684593, at *5 (E.D. Tenn. Aug. 25, 2022); *see also* Fed. R. Crim. P. 41(e)(2), Advisory Committee Note, 2009 Amendments ("A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs."). The Government is unaware of any judicial decision that reaches a contrary position.

Here, Purbeck's iPhones were seized from his residence on August 21, 2019—two days after the search warrant was signed by Judge Bush on August 19, 2019. (Doc. 87 at 67–68.) Therefore, under the plain text of Rule 41(e)(2), the search warrant was timely executed in accordance with the Federal Rules of Criminal Procedure.

Purbeck's reliance on *United States v. Vedrine*, 2022 WL 17259152 (11th Cir. Nov. 29, 2022), is misplaced.[4] *Vedrine* in fact rejected the defendant's contention of unreasonable delay between the execution of a search warrant by copying data from a phone seized incident to arrest and the subsequent forensic examination of that device. *Id*. at *5. In that context, the Eleventh Circuit's unpublished, *per curiam* decision in *Vedrine* recognized the settled proposition that the warrant had been executed at the time that law enforcement had copied the contents of the phone. *Id.* Indeed, under the plain language of the rule, law enforcement can

[4] Even if Purbeck had not misread *Vedrine*, it is not clear that Eleventh Circuit law would govern the execution of the search of devices seized from Purbeck's Idaho residence. (*See* Doc. 96 at 14 n.5 (expressing that the district court was inclined to apply Ninth Circuit law under the *lex loci* approach.))

execute a search warrant for electronically stored information by seizing a device pursuant to a premises warrant and can also do so by copying that information. Fed. R. Crim. P. 41(e)(2)(B) ("The time for executing the warrant in Rule 41(e)(2)(A) . . . refers to the seizure or on-site copying of the media or information . . .").

In his motion, Purbeck focuses on one sentence in the *Vedrine* opinion, namely: "Based on the plain language of the rule, we agree with our sister circuits that once the data is seized and extracted by law enforcement, the warrant is considered executed for purposes of Rule 41 . . ." 2022 WL 17259152, at *6. But Purbeck misreads this sentence to hold that, despite the plain language of Rule 41, a warrant for electronic information is only executed when data is extracted from the device. (Doc. 99 at 4.) The Government is unaware of any such holding in *Vedrine* or elsewhere.

Tellingly, the two cases that the *Vedrine* decision quotes in support of the sentence at issue hold the *exact opposite* of Purbeck's proposed reading—both cases conclude that a warrant is executed at the time of the seizure of an electronic device. *See United States v. Cleveland*, 907 F.3d 423, 431 (6th Cir. 2018) ("[T]he district court held, and we agree, the November 6 warrant's execution date set a deadline only for when the physical cellphone itself had to be seized, and not for when its data were to be extracted."); *United States v. Huart*, 735 F.3d 972, 974 n.2 (7th Cir. 2013) ("[U]nder Federal Rule of Criminal Procedure 41€(2)(B), a warrant for electronically stored information is executed when the information is seized or copied—here, when the Rock Valley staff seized the phone. Law enforcement is permitted to decode or otherwise analyze data on a

seized device at a later time."). In a word, because Purbeck's motion is grounded on a misreading of the holding of *Vedrine*, his motion to suppress should be denied.

B. Purbeck's challenge to the reasonableness of the iPhone review is untimely.

In addition, Purbeck also argues, irrespective of when the search warrant was executed, that the review of the iPhone 7 and iPhone 8 seized from his residence was unconstitutionally unreasonable. (Doc. 99 at 6.) This argument is untimely and waived.

Under Federal Rule of Criminal Procedure 12, a defendant must raise a motion to suppress evidence prior to trial and within the deadline set by the Court. Fed. R. Crim. P. 12(b)(3)(C) & 12(c). If a motion to suppress is not timely raised, the party waives the defense unless the defendant shows good cause. Fed. R. Crim. P. 12(c)(3); *see also United States v. Mwangi*, No. 109-CR-107-TWT, 2010 WL 520793, at *5 (N.D. Ga. Feb. 5, 2010).

Here, Purbeck's pretrial motions were due on December 13, 2021. (Doc. 24.) And indeed, Purbeck filed a number of motions which were briefed and litigated in this case. While Purbeck has explained that his counsel has only recently learned of the November 2022 *Vedrine* decision, that does not explain his failure to challenge the search of the iPhones until July 2023—after lengthy initial pretrial briefing, an evidentiary hearing, post-hearing briefing, Judge Vineyard's Report and Recommendation, and the filing of Purbeck's objections to the Report and Recommendation. Absent a showing of good cause, which is not set forth here, Purbeck's argument as to the reasonableness of the review of the iPhones should be deemed waived as untimely. *Mwangi*, 2010 WL 520793, at *5 ("Neither

the government nor the Court were on notice that [defendant] challenged his statements as fruits of a purported Fourth Amendment violation and he will not be heard to raise such a claim after the evidentiary hearing record is closed.").[5]

C. The Government made reasonable efforts to decrypt and review the iPhones at issue.

Purbeck alleges that the Government "took no steps to access the I-phone 8 and the I-phone 7 from August 21, 2019 until May 30, 2023. . ." (Doc. 99 at 4.) Even putting aside that this statement is inaccurate, Purbeck's threadbare allegation that the Government's review of his cellphones was unreasonable fails to carry his burden as required for a motion to suppress. *United States v. Touset*, 890 F.3d 1227, 1231 (11th Cir. 2018) ("[T]he individual challenging the search bears the burdens of proof and persuasion.") (quoting *United States v. Newsome*, 475 F.3d 1221, 1224 (11th Cir. 2007)). In his motion, Purbeck only alleges a "generalized time grievance and puts forth no persuasive evidence of unreasonable action[.]" *Vedrine*, 2022 WL 17259152, at *6. Nor does he make any argument that the probable cause that justified the warrant went stale or dissipated because of the time of review. *See United States v. Nicholson*, 24 F.4th 1341, 1351 (11th Cir. 2022).

[5] Purbeck also seeks to "incorporate[] by reference the arguments he previously made in his motions to suppress and post-hearing briefs[.]" Judge Batten already rejected the arguments previously raised (Doc. 96,) and those arguments were not properly presented here. *See, e.g.*, *Davis v. DeKalb Cnty., Georgia*, No. 1:03-CV-2853-WSD, 2005 WL 8154356, at *2 (N.D. Ga. May 31, 2005) (quoting *Four Seasons Hotels and Resorts v. Consorcio Barr, S.A.*, 377 F.3d 1164, 1167 n.4 (11th Cir. 2004)).

In the end, Purbeck has not made a *prima facie* showing that the Government took unreasonable steps in reviewing the locked iPhones at issue. "Although the government has not completed the review and seizure of all records authorized by the warrant[], it has not violated the terms of the warrant[] by not doing so." *United States v. Lee*, No. 1:14-CR-227-TCB-2, 2015 WL 5667102, at *15 (N.D. Ga. Sept. 25, 2015). The Eleventh Circuit has recognized in the context of warrant particularity that "the magnitude of the search . . . is not sufficient to establish a constitutional violation." *United States v. Sawyer*, 799 F.2d 1494, 1509 (11th Cir. 1986) (citing *United States v. Wuagneux*, 683 F.2d 1343, 1352 (11th Cir. 1982)). "Instead, the search 'may be as extensive as reasonably required to locate and seize items described in the warrant.'" *Id.*; *see also United States v. Sedlak*, 697 F. App'x 667, 668 (11th Cir. 2017) ("We have recognized that effective investigation of complex white collar crimes may require 'the assembly of a 'paper puzzle' from a large number of seemingly innocuous pieces of individual evidence,' and that the complexity of a crime cannot be used as a shield against detection when the government has shown probable cause that a suspect possesses evidence of a crime.'") (internal citations omitted).

Moreover, Purbeck provides no relevant authority in support of his contention that the Government's review of the encrypted and voluminous electronic materials in this cybercrime investigation was unreasonable. Rather, he seems to rely on *Vedrine*, where the Eleventh Circuit rejected the argument that any later review was unreasonable and adopted the view in the Rule 41 Advisory Committee Notes that review of electronic evidence can take a "substantial amount of time." *Vedrine*, 2022 WL 17259152, at *6. The Advisory

Committee Notes specifically acknowledge the reasons for delay at issue, including encrypted devices and law enforcement resource constraints. Fed. R. Crim. P. 41(e)(2), Advisory Committee Note, 2009 Amendments.

Even though he misreads *Vedrine*, Purbeck yet acknowledges that Judge Batten's decision in *United States v. Dixon* is persuasive authority that runs directly contrary to his position. (Doc. 99 at 4;) No. 3:20-CR-3-TCB, 2021 WL 1976679, at *2 (N.D. Ga. May 18, 2021) (finding delay in review based on locked phones and resource constraints reasonable). Indeed, in *Dixon*, the fact that the defendant's iPhone was locked with a passcode and the defendant did not provide the agents with a passcode was itself sufficient for the delay in reviewing the device. *Id*. Purbeck then attempts to distinguish *Dixon* by arguing that "[i]n contrast to *Dixon*, Mr. Purbeck had provided his passwords to the Government." (Doc. 99 at 4.) But the fact that Purbeck provided passwords to certain email accounts is immaterial to the Government's inability to access Purbeck's iPhones— to which he did not provide the passcodes. *See* Fed. R. Crim. P. 41(e)(2), Advisory Committee Note, 2009 Amendments (recognizing the reasonable delays arising from "difficulties created by encryption").

Purbeck also cites *United States v. Mitchell* for the proposition that the government cannot keep computers or electronics without lawful grounds. (Doc. 99 at 6–7 (quoting 565 F.3d 1347, 1350–51 (11th Cir. 2009).) But *Mitchell* is also distinguishable as it considered the retention of electronic devices seized from a home *without* a warrant—a situation clearly inapplicable to Purbeck's iPhones, which were lawfully seized pursuant to a search warrant. *Id*. at 1351; *see also United States v. Ilonzo*, No. 1:12-CR-276-SCJ-GGB, 2015 WL 5827598, at *20 (N.D.

Ga. Oct. 6, 2015) (citations omitted). Thus, the additional limitations on a warrantless seizure of property from a home, which is presumptively unreasonable, *Kentucky v. King*, 563 U.S. 452, 459 (2011), are not relevant to the evidence here lawfully seized pursuant to a warrant.

Finally, Purbeck cites an outlier case, *United States v. Metter*, 860 F. Supp. 2d 205 (E.D.N.Y. 2012), that only reinforces the reasonableness of the Government's review of the encrypted iPhones here. In *Metter*, in the context of the retention of potentially privileged information, the court found that the government's retention of data "without any review whatsoever" for "relevance" or "privilege" was "unreasonable," where "the government . . . failed to commence the review, despite repeated requests from defense counsel and directions from the Court to do so." *Id.* at 215-16. Accordingly, a number of courts, including this Court, have distinguished *Metter* based on its unique fact pattern, which involved no encryption-related delays. *See Dixon*, 2021 WL 2327063, at *6 (N.D. Ga. Apr. 15, 2021) ("*Metter* did not 'involve a delay caused by encryption difficulties,' as in this case."); *see also United States v. Jarman*, 847 F.3d 259, 267 (5th Cir. 2017); *United States v. Manafort*, 314 F. Supp. 3d 258, 272 (D.D.C. 2018); *United States v. Manafort*, 2018 WL 3383021, at *9 (E.D. Va. July 10, 2018).

In sum, the Government here took reasonable steps consistent with the Federal Rules of Criminal Procedure and the Fourth Amendment to review the encrypted iPhones at issue, and therefore Purbeck's challenge of an unreasonable time for that review fails to meet his burden and should be denied.[6]

[6] Indeed, the FBI is still attempting to decrypt several other password-protected storage devices seized from Purbeck's residence. If the FBI is

D. Even if the duration of the review was unreasonable, suppression is not an appropriate remedy.

Even assuming *arguendo* that the review of the devices was unreasonably delayed, suppression of the iPhone evidence would not be warranted.

As this Court has observed, "'[e]xclusion of evidence is an extreme sanction to be used only as a 'last resort,' and to 'trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.'" *Dixon*, 2021 WL 2327063, at *8 (*quoting United States v. Brooks*, 648 F. App'x 791, 794 (11th Cir. 2016)) (internal quotations omitted). Instead, courts have repeatedly declined to suppress delayed forensic reviews absent prejudice to the defendant by the delay or intentional and deliberate disregard of Federal Rule of Criminal Procedure 41. *See id*; *see also United States v. Nicholson*, 24 F.4th 1341, 1351–52 (11th Cir. 2022) (determining that a belated search of electronically stored images on a laptop in police custody did not warrant suppression due to lack of prejudice or intentional or deliberate disregard for the law); *United States v. Lee*, No. 1:14-CR-227-TCB-2, 2015 WL 5667102, at *15 (N.D. Ga. Sept. 25, 2015) (rejecting suppression based on prolonged forensic review where "the government has not flagrantly disregarded the terms of the warrant[.]"); *United States v. Alston*, No. 15 CR. 435 (CM), 2016 WL 2609521, at *4 (S.D.N.Y. Apr. 29, 2016) (concluding that "suppression would not be the appropriate remedy [for an unreasonable delay] because there was no prejudice

---

successful, the Government will timely provide the images to Purbeck as part of its ongoing discovery obligations.

to the defendant by the delay, and there is no evidence of any intentional and deliberate disregard of any provision of Rule 41.").

In this case, Purbeck has not plausibly alleged any grounds for finding that he was prejudiced by the delayed review nor that the Government has intentionally or deliberately disregarded the requirements in Rule 41. Thus, even if the Government's delay in reviewing the iPhones was unreasonable, Purbeck has not provided a basis for the requested "extreme sanction" of suppressing the evidence from these lawfully seized password-protected devices.

E. Purbeck's motion does not warrant an evidentiary hearing.

It is uncontested that the Government has only recently unlocked the iPhone 7 and iPhone 8 at issue in Purbeck's motion. The Government timely produced the images of the phones and Purbeck now has that evidence as supplemental discovery. The Government submits its review was reasonable, but even if it was not, the extreme sanction of suppression would still be unwarranted. Therefore, this Court should decline to "grant [Purbeck] an evidentiary hearing so that he may go on a fishing expedition for indicia of unreasonableness." *United States v. Sosa*, 379 F. Supp. 3d 217, 222 (S.D.N.Y. 2019). Purbeck's motion should be denied.

Conclusion

For the foregoing reasons, the Court should deny Purbeck's motion to suppress the evidence from the search of his iPhone 7 and iPhone 8.

Respectfully submitted,

RYAN K. BUCHANAN
United States Attorney

Michael Herskowitz
/s/MICHAEL HERSKOWITZ
ASSISTANT UNITED STATES ATTORNEY
Georgia Bar No. 349515
600 U.S. Courthouse
75 Ted Turner Dr. SW
Atlanta, GA 30303
404-581-6000
michael.herskowitz@usdoj.gov

ALEX R. SISTLA
Assistant United States Attorney
Georgia Bar No. 845602
alex.sistla@usdoj.gov

NATHAN P. KITCHENS
Assistant United States Attorney
Georgia Bar No. 263930
nathan.kitchens@usdoj.gov

BRIAN Z. MUND
Trial Attorney, U.S. Department of Justice
Computer Crime and Intellectual Property Section
CA Bar No. 324699
Brian.Mund@usdoj.gov